

From: [redacted]
Sent: Tuesday, January 02, 2007 1:59 PM
To: Taskforcecomments
Subject: Identify Theft Task Force Public Comment

Gentlemen:

Despite efforts on my family's part (keeping social security numbers as secure as possible; shredding all personal information; etc) we have been notified twice that my husband's personal information has been compromised. Once by the the veteran's administration in the much publicized laptop theft and most recently by a company from which he receives a pension. In the latter instance all of his personal information is contained on a file in a laptop computer that was stolen from an employee. While we were notified in a timely manner and efforts by the government agency and the private sector company to give us information on monitoring our credit and unauthorized use of the personal information, it does NOT ensure that we will not be victims of identify theft because of the careless exposure of our personal information. If our information is compromised it will be incumbent upon us to rectify the countless inconveniences it may cause.

I feel that there must be stronger consequences for those who compromise personal information whether knowingly or unknowingly. While I am sure that the individuals that had their computers stolen did not expect to cause untold inconveniences and distress for thousands, that is the result of their carelessness.

One step that I feel the task force must address is the common use of Social Security numbers as a means of identification linked to credit. There must be another way to identify individuals. Printed on my Social Security card is the statement "for social security and tax purposes - not for identification". When did that statement become obsolete?

Also, I believe the task force must address the terrible inconvenience that surrounds the reclaiming of one's identity. The process can take years and have unforeseen consequences for unsuspecting victims.

Another concern is the casual way information is handled. The computer that was stolen in the second instance was in an employee's car. I believe that sensitive information should NEVER physically leave the establishment that has been entrusted with that information. Businesses, government agencies and their employees should be held accountable for any breech of security regarding an individual's identity.